IP Security & DNS Security: Overview & Status

Randall Atkinson

<rja@inet.org>

Outline

- Internet Document Types
- IP Security (IPsec)
  - Technology & Status
- DNS Security (DNSsec)
  - Technology & Status
- Summary

Internet Documents

- *Internet-Draft*
  - unapproved working drafts; anyone may write.
- *Proposed Standard RFC*
  - requires stable,clear technical specification.
- *Draft Standard RFC*
  - requires demonstrated interoperability.
- *Full Standard* RFC
  - requires demonstrated significant deployment.

IP Security

IP Security Architecture

- Two separate IP security mechanisms.
- AH only provides authentication.
- ESP provides confidentiality with optional authentication.
- Decoupled key management.
- Security Associations are created by key management for AH/ESP sessions.

IPsec Security Association

- Security Parameters Index (SPI)
- Source Address
- Destination Address
- Source Identity
- Destination Identity
- Sensitivity Label
- {other attributes}
- Security Protocol
- Crypto Algorithm(s)
- Algorithm mode(s)
- IV/CryptoSync
- SA “soft” Lifetime
- SA “hard” Lifetime
- Replay Protection

Security Parameters Index (SPI)

- Receiver uses (SPI, Destination Address) to locate the correct Security Association.
- The SPI is an opaque 32-bit field.
- Most SPI numbers are sparsely allocated.
- The SPI can be used to distinguish different concurrent sessions between the same (Source, Destination) nodes.

Lifetimes

- Each Security Association has a lifetime.
- Lifetimes could be based on:
  - clock time the SA lives once use has begun
  - usage in bits protected by this SA
  - usage in packets sent/received.
- Lifetime of a SA might be shorter than the lifetime of the IP session using the SA.

Identity Types

- IPv4 Address (“132.250.90.1”)
- IPv4 Address Range (“132.250.0.0/16”)
- IPv6 Address (“ABCD::0001”)
- IPv6 Address Range (“ABCD::0/64”)
- Fully Qualified Domain Name (“inet.org”)
- Mailbox Name (“rja@inet.org”)

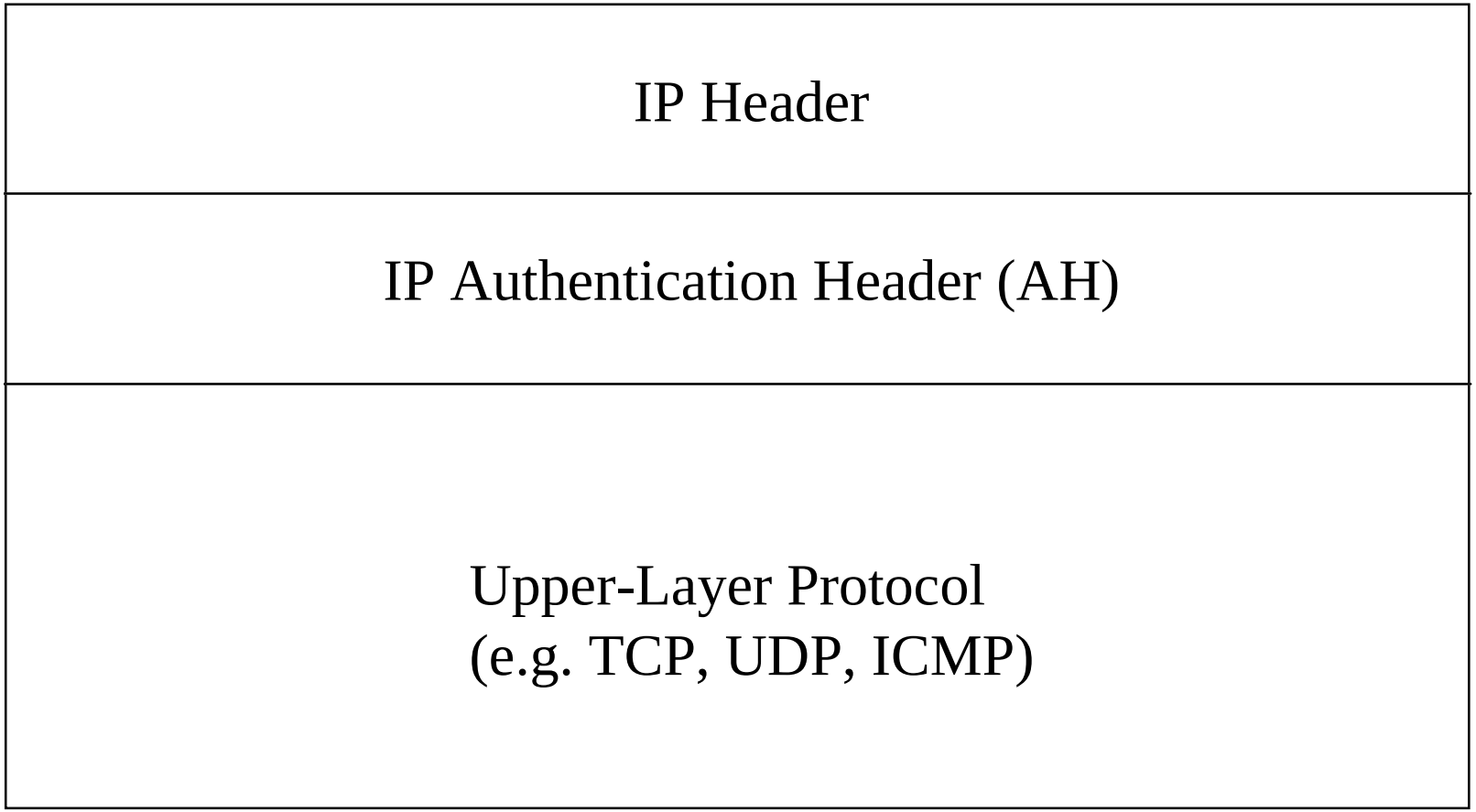
Sensitivity Label

- Not always present.
- Indicates sensitivity of transmitted data.
- Useful in commercial as well as governmental contexts.
- Sensitivity of data will usually impact the key management approach/options selected.

IP Authentication Header

- Provides cryptographic authentication without confidentiality.
- Algorithm-independent
- Default algorithms are:
  - Keyed HMAC MD5
  - Keyed HMAC SHA-1
- Replay Protection available.

Example IP Packet with AH



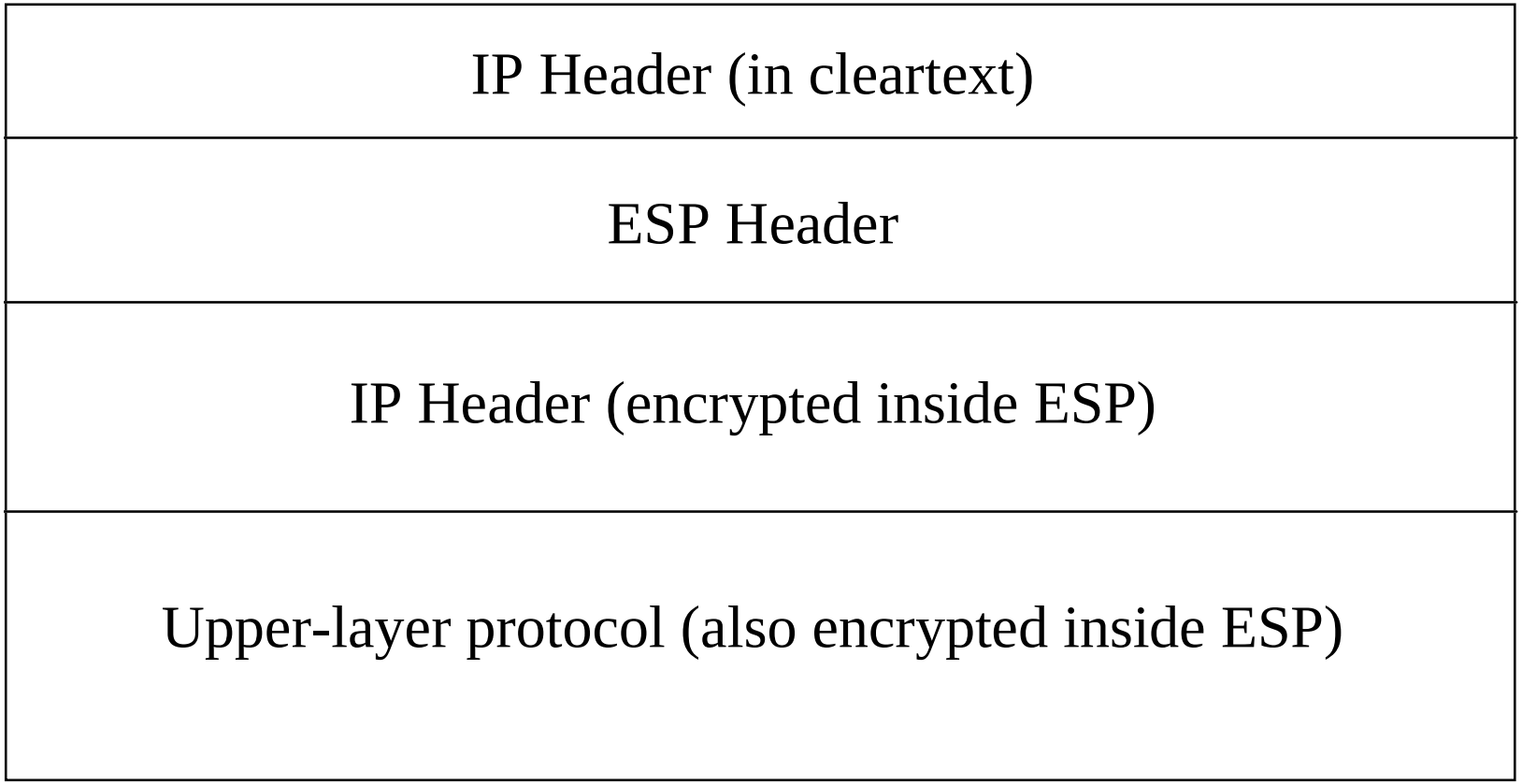
ESP Overview

- Provides confidentiality through encryption.
- Provides authentication/integrity also.
- Algorithm-independent.
- Optional-to-use Replay Protection.
- Default algorithm:
  - DES-CBC with HMAC-MD5 and Replay Prot.

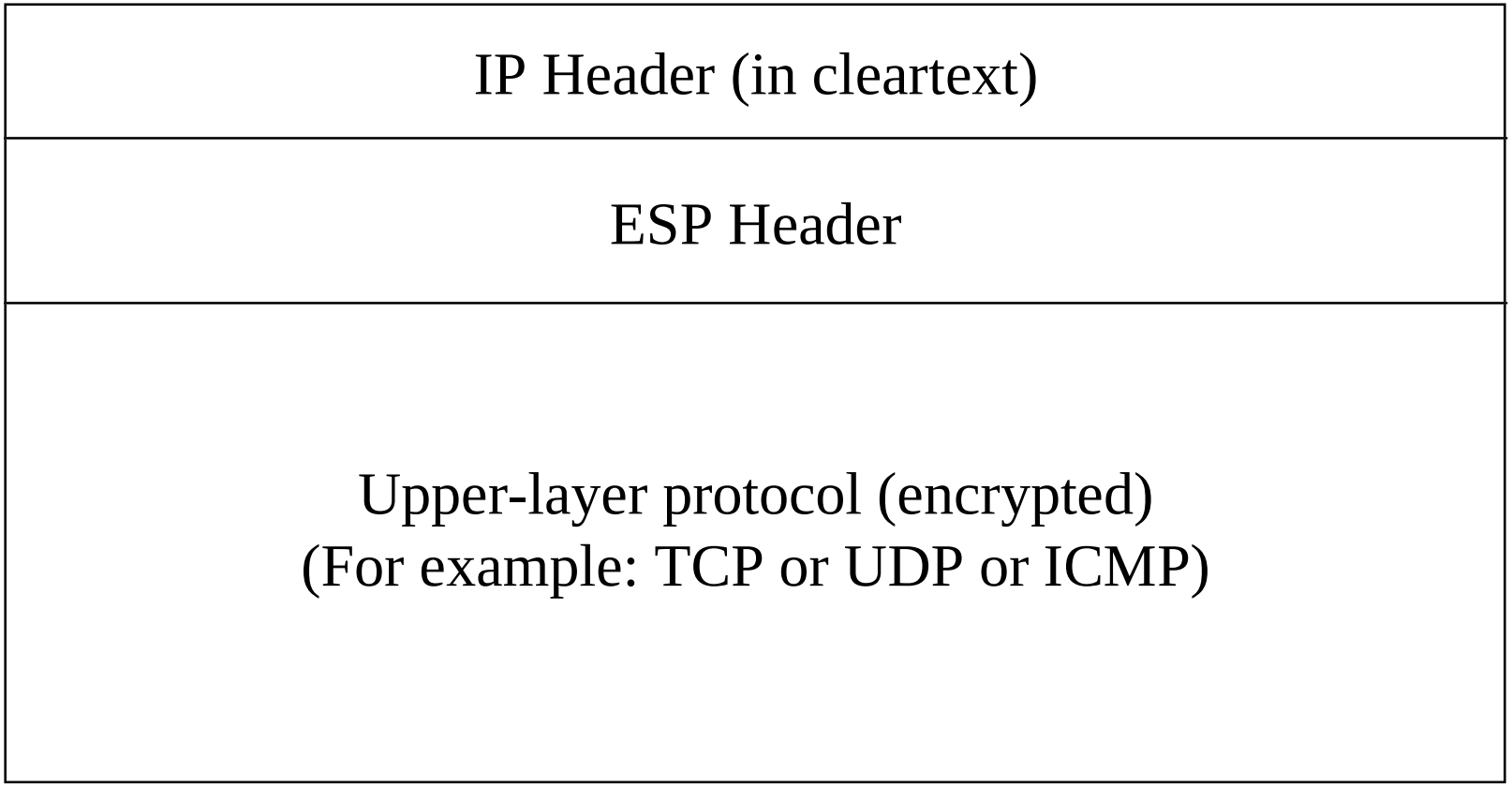
ESP Modes

- Modes are useful abstractions that don't change packet processing very much.
- Tunnel Mode
  - Encapsulates entire IP datagram inside ESP header and a prepended cleartext IP header.
- Transport Mode
  - Only encapsulates upper-layer protocol inside ESP and leaves original IP header as cleartext.

Example ESP Tunnel Packet



Example ESP Transport Packet



Combined ESP Transform

- Mandatory-to-implement default transform.
- DES-CBC for encryption.
- HMAC-MD5 for integrity/authentication.
- Replay Protection via 64-bit counter.
- Replaces older insecure ESP transform.

Public Key Certificates

- Likely to be used by IPsec key management
- Authenticates binding between the *principal* and the principal's *public key*.
- Common examples include:
  - Signed keys from Secure DNS.
  - X.509 Version 3.
  - PGP Keys.

Types of Key Management

- Out-of-Band (e.g. ISAKMP)
- In-Band (e.g. Sun's SKIP)
- Manual

IPsec Standards Status

- Basic ESP/AH published as Proposed Standard RFCs in August 1995.
- Specifications likely to be published as standards-track RFCs in Spring 1998:
  - Revised ESP/AH base specifications.
  - Revised ESP/AH transforms.

IPsec Summary

- ESP provides encryption and authentication.
- AH provides authentication w/o encryption.
- Key Management is an essential, but separately specified component.
- IETF specifies the mechanisms, but users need to consider and specify appropriate security policies

DNS Security

DNS Security

- Provides authentication for information stored within the Domain Name System (DNS).
- Extends DNS to permit storage of signed public keys in addition to IP addresses and domain names.

DNS Authentication

- Provides authentication for data stored within the Domain Name System.
- Cryptographic Algorithms:
  - Originally specified RSA, which is patented.
  - Revised to use DSA, which is freely available.
- Uses the new “SIG” record to hold signatures for the DNS data being protected.

Key Distribution via DNS

- DNSsec extension that permits distribution of signed public keys.
- Key may be bound to any DNS record:
  - Domain Name.
  - "*A*" or "*AAAA*" records for IP address.
  - "*MB*" record for mailbox identities.
- Uses the new *KEY* DNS record type.

Key Distribution Issues

- IETF has multiple groups working on public key infrastructure (SPKI, PKIX).
- DNSsec's *KEY* record doesn't use X.509.
- X.509 will be obtainable via *Lightweight Directory Access Protocol (LDAP)*.
- Hence, no single source for all forms of public key information.

Key Exchanger (KX) Record

- Published as Informational RFC-2230.
- Status:
  - Not on the IETF standards-track at present
  - Being implemented by several vendors.
- Defines *KX* record type and semantics.
- Can help identify security gateways.
- Can facilitate Proxy Key Management.

DNS Security Standards

- Basic DNSsec published January 1997 as Proposed Standard RFC-2065.
- Revised DNSsec specifications expected to be published in first half of 1998.
- Freely distributable BIND integration with DNSsec is in progress.
- DNSsec has already been granted export approval since it is authentication-only.

Summary

Standards Status

- IPsec specifications are nearly complete.
- IPsec products are becoming available.
- DNSsec specifications are nearly complete.
- DNSsec is becoming available.
- IPsec key management can leverage signed public keys from DNSsec.

Technology Maturity

- Vendor implementations starting to appear.
- Vendor interoperability is still weak.
- More deployment experience is needed.
- More operational experience is needed.
- Security Testbeds using research networks (e.g. ESnet, DREN) can help provide that needed experience and feedback to IETF.

Residual Risks

- Perfect Security is unobtainable.
- Quality of implementation varies.
- Keys must be protected.
- OS and implementation-specific vulnerabilities remain an issue.
- Will need to change cryptographic algorithms over time.